Department for
Digital, Culture
Media & Sport

A New Data Protection Bill: Our Planned Reforms

Statement of Intent

7 August 2017

Contents

Ministerial Foreword

The Rt Hon Matt Hancock MP
Minister of State for Digital

A generation ago Parliament passed the Data Protection Act. Since then, digital technology has transformed almost every aspect of our lives. This has brought huge advantages: social advantage, bringing the world closer together, and economic advantage, transforming our economy. For all its many benefits, there are also concerns. Parents worry that their children may be vulnerable online in ways they don't understand. Customers worry what companies are doing with their data. Citizens worry that others might intrude on their privacy online.

To protect people's privacy, while allowing and encouraging the innovation that digital technology allows, we must balance freedom and responsibility online. The Data Protection Act has done this well, providing us with more control over how our personal information is used and limiting processing to the purpose for which it was collected, subject to various public interest exemptions. We have stronger protections in the UK than most, and our regulatory arrangements are often seen as the gold standard. While we should all be assured that data is well protected in the UK, change is needed. The technology, and society has changed.

The Data Protection Bill, promised in our manifesto and announced in the Queen's speech, will bring our data protection laws up to date. It will both support innovation by ensuring that scientists and businesses can continue to process data safely. It will ensure that we can remain assured that our data is safe as we move into a future digital world based on a system with more accountability, but less bureaucracy. The Bill includes tougher rules on consent, rights to access, rights to move and rights to delete data. Enforcement will be enhanced, and the Information Commissioner given the right powers to ensure consumers are appropriately safeguarded.

The Bill will also bring EU law into our domestic law. On 23 June 2016, the EU referendum took place and the people of the United Kingdom voted to leave the European Union. Until exit negotiations are concluded, the UK remains a full member of the European Union and all the rights and obligations of EU membership remain in force. During this period the government will continue to negotiate, implement and apply EU legislation. The outcome of these negotiations will determine what

arrangements apply in relation to EU legislation in future once the UK has left the EU.

Bringing EU law into our domestic law will ensure that we help to prepare the UK for the future after we have left the EU. The EU General Data Protection Regulation (GDPR) and the Data Protection Law Enforcement Directive (DPLED) have been developed to allow people to be sure they are in control of their personal information while continuing to allow businesses to develop innovative digital services without the chilling effect of over-regulation. Implementation will be done in a way that as far as possible preserves the concepts of the Data Protection Act to ensure that the transition for all is as smooth as possible, while complying with the GDPR and DPLED in full.

When it comes to law enforcement, the Bill will ensure that the data of victims, witnesses and suspects of crimes, are protected in the context of criminal investigations and law enforcement action. It will ensure that criminal justice agencies can continue to tackle crime and terrorism whilst protecting the data rights of those involved in criminal investigations or proceedings. Criminals and terrorists show no respect for international borders so the Bill will ensure that UK criminal justice agencies work effectively with counterparts in other countries.

The Data Protection Bill will allow the UK to continue to set the gold standard on data protection. We already have the largest internet economy in the G20. This Bill will help maintain that position by giving consumers confidence that Britain's data rules are fit for the digital age in which we live.

Matt Hancock

1. The Digital Economy

Supporting our data economy

More data is being produced than ever before. Our connected world brings many benefits like being able to stay in touch with friends and relatives around the world and underpins our prosperity, with millions of jobs and billions of value directly linked to the internet. Of the G20 countries we have the largest internet economy as a percentage of GDP and have extended that lead since it was first measured[1].

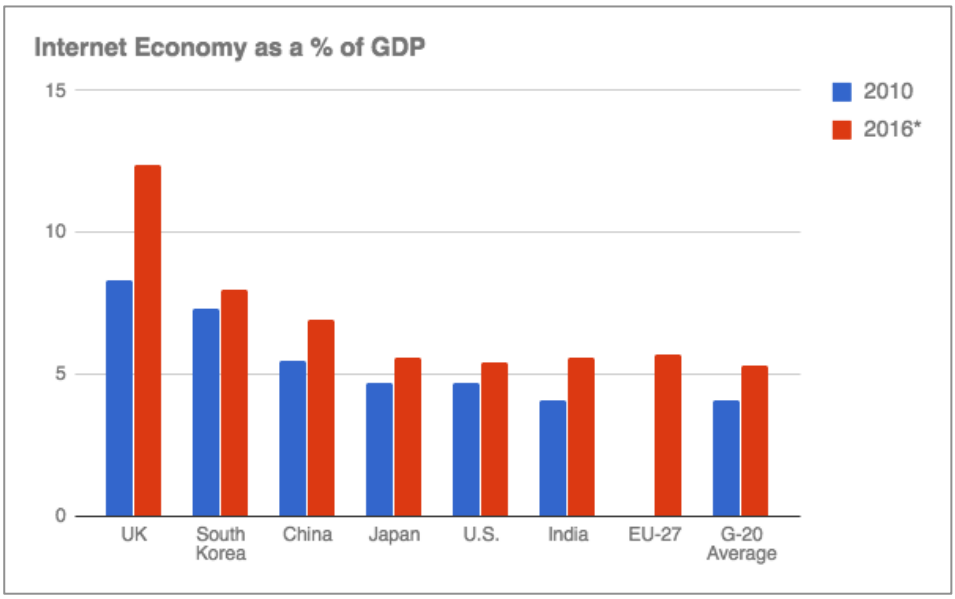

*Fig: BCG Internet Economy in the G-20 Report (2012), * 2016 are projected figures from when it was measured in 2012* [2]

This brings massive economic benefits, in terms of investment and employment. Of the 30 cities in the European Digital City Index of the best places for tech startups, nine are in UK.[3]

Our technology industry thrives because of access to skills, infrastructure and investment but also, importantly, because we have a population that has adopted the internet as a place to transact. Our innovative engagement with the internet makes the UK a world-beating customer-base for those developing digital industries.

Our digital economy is creating mind-boggling quantities of personal data. At the same time, radically lower costs of collection, storage and processing - coupled with

[1] Boston Consulting Group (2015), https://www.bcg.com/d/press/1may2015-internet-contributes-10-percent-gdp-uk-economy-12111
[2] https://www.bcg.com/documents/file100409.pdf
[3] https://digitalcityindex.eu/
[2] https://www.bcg.com/documents/file100409.pdf
[3] https://digitalcityindex.eu/

rising computing power - are making this data a rich raw material. This is creating new opportunities for business growth across all industry sectors, changing how we innovate, market, sell and consume services.

Our data economy will be integral to the UK's growth and future prosperity. Analysis predicts that data will benefit the UK economy by up to £241 billion between 2015 and 2020[4]. Our digital strategy, therefore, will ensure businesses and Government are able to use data in innovative and effective ways. This includes creating a strong data infrastructure, having a high level of regulatory compliance, developing a data-literate workforce, and increasing the number of people with advanced data skills.

Protecting data

Our vision is to make the UK the safest place to live and do business online. With the increasing volumes of personal data there is an increasing need to protect it. Data loss can have distressing repercussions on individuals whilst risking significant reputational damage for the responsible party. Victims lose trust. In more serious cases significant financial loss can arise on both sides and there are risks of other serious harms. Protecting data is a global concern and the UK is at the forefront of innovation in this area.

The Data Protection Act 1984 established the Data Protection Registrar, replaced by the Information Commissioner in the Data Protection Act 1998. The Commissioner is an independent official whose role is to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner investigates complaints as well as conducting proactive investigations. As well as an enforcer, the Commissioner acts to inform and educate data controllers to improve standards.

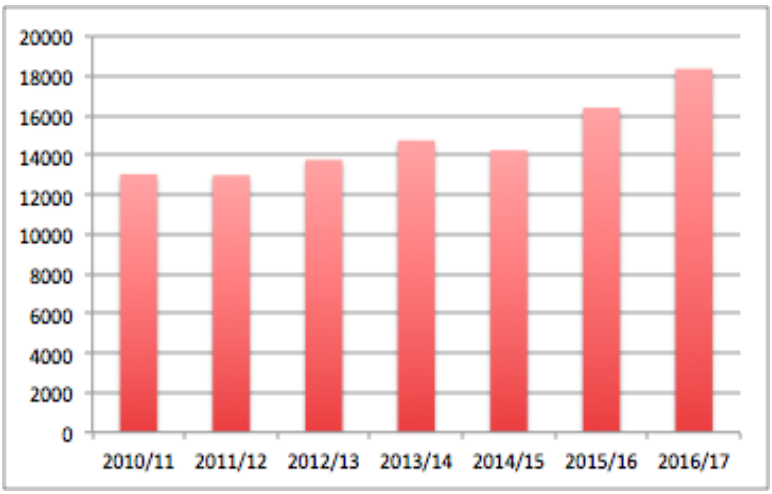

Fig: Data protection concerns received by the Information Commissioner for each financial year (source: ICO annual reports)

[4] The Value of Big Data and the Internet of Things to the UK Economy, Feb 2016, CEBR & SAS

The Data Protection Act 1998, which provides the legal framework for the use of personal data, is often cited as a global gold standard. In 2010 the Commissioner was given new teeth with the power to enforce fines and further powers have been given incrementally, most recently in the Digital Economy Act 2017, which made it easier to enforce the law against those who make nuisance calls. The Data Protection Act needs to be kept up to date for a changing world, to maintain public confidence in the face of "big data" and all the arrays of other technological developments that we benefit from all the time. We all have so much online data that we have created or others have collected that we need to be equipped to exercise our rights over it.

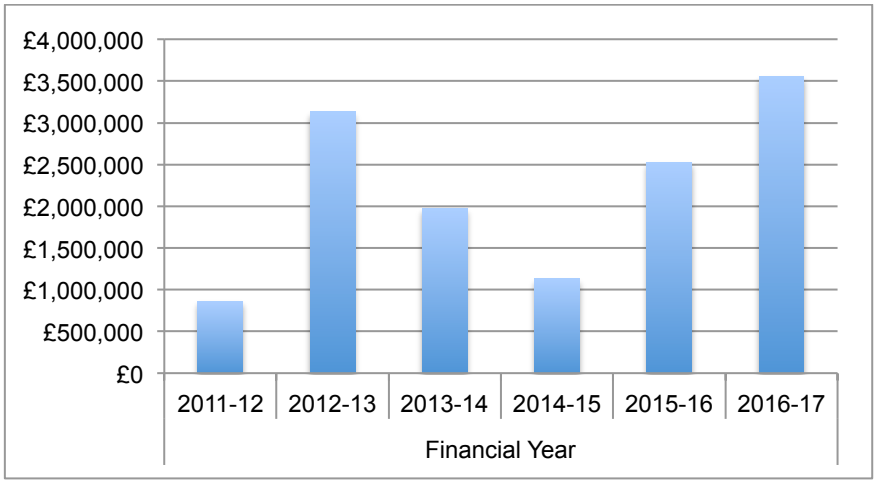

Fig: fines issued by the Information Commissioner under the Data Protection Act and Privacy of Electronic Communication Regulations

The right legal frameworks are, of course, only part of the effort that government puts into protecting data. We also work with the Information Commissioner and consumer groups to educate people about how to protect themselves. We are also securing the country from cyber attacks and last year established the National Cyber Security Centre (NCSC) to help protect our critical services from cyber attacks, manage major incidents and improve the underlying security of the internet through technological improvement and advice to citizens and organisations. The NCSC works together with UK organisations, businesses and individuals to provide authoritative and coherent cyber security advice and cyber incident management. This is underpinned by world class research and innovation.

Our objectives

To fulfil our vision of being the best, and safest, place to live and do business online, we have three inter-related objectives.

1. Maintaining Trust

For the UK to benefit fully from the economic and social gains of data innovation, the

public needs to know that their personal data is safe and used responsibly.
Institutions must maintain the confidence and trust of those who provide their data by ensuring that:

- data will be kept safe and secure;
- data will be handled legally, responsibly and ethically;
- people are open and transparent about what data they are using and why; and,
- strict penalties will apply for misuse.

2. Future trade

The ability to transfer data across international borders is crucial to a well functioning economy. We are committed to ensuring that uninterrupted data flows continue between the UK, the EU and other countries around the world. The Data Protection Bill will place us on the front foot in allowing the UK to maximise future data relationships with the EU and elsewhere.

3. Security

The ability to collect, share and process personal data is crucial not only for the economy, but also for our security and law enforcement.

Criminals do not respect international borders, therefore our law enforcement efforts need to be dynamic in order to tackle modern crime threats. As part of our plans for the UK's exit from the EU, we will consider carefully how best to maintain our ability to share, receive and protect data with other EU Member States.

In a connected society criminal justice agencies need to share data with each other, and with other partners in both the public and private sector and embrace technology as a tool for preventing and detecting crime. While the criminal justice agencies do their important work, we must ensure they operate within a data protection regime that continues to build a culture of data confidence and trust.

2. Our Data Protection Reforms

Overview

We will ensure that the UK's data protection framework continues to protect personal data in our new digital age. We will enhance protections by allowing citizens much greater control of their own data.

Alongside strengthening individuals' rights, we will offer further clarity and certainty to businesses whilst they continue to collect, share and process personal data - in so doing maintaining the UK's world-renowned culture of innovation, promoting economic growth and cementing the UK's position as a global leader in the digital economy.

Personal data is information that is attributable to an individual and may help to identify them. We will expand the definition of 'personal data', reflecting the growth in technology over the past 20 years to include IP addresses, internet cookies and DNA.

Protecting individuals

We will protect privacy, strengthen rights and empower individuals to have more control over their personal data by providing easier access.

Individuals will generally have more control over their digital footprint, their personal data, how it is used and passed on by companies. Specifically, UK citizens will be better protected by a combination of new and strengthened existing rights:

- Privacy: the rules around consent are being strengthened and subject to additional conditions, such as being 'unambiguous' and easy to withdraw. Consent must also be 'explicit' when processing sensitive personal data.

  We will ensure that the default reliance on the use of default opt-out or pre-selected "tick boxes" - which are, in any case, largely ignored - will become a thing of the past. We will require parents or guardians to give consent to information services[5] where a child is under the age of 13. We will make it simple to withdraw consent.

- Improved data access: individuals will find it easier to require an organisation to disclose the personal data it holds about them at no charge[6].

[5] Information services comprise any service normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data, and at the individual request of a recipient of a service.
[6] Subject to the understanding that such requests are not "manifestly unfounded or excessive."

People cannot determine whether information held about them is correct if they do not know what information is held. Data controllers will provide better information on how to access information and empower people to take ownership.

- Data portability: new rules will make it easier for customers to move data between service providers; this not only gives consumers greater choice, but will promote competition and innovation in a range of sectors.

  Where you change internet service provider, if you are using email or file storage services to store personal photographs or other personal data you should be able to move that data.

- Right to be forgotten: individuals will be able to ask for their personal data to be erased[7]. This will include provision to allow people to require social media platforms to delete information they posted during their childhood.

  In certain circumstances, individuals will have the ability to ask social media companies to delete any or all of their posts. For example, a post on social media made as a child would normally be deleted upon request, subject to very narrow exemptions.

- Profiling: individuals will have greater say in decisions that are made about them based on automated processing. Where decisions are based on solely automated processing individuals can request that processing is reviewed by a person rather than a machine.

Protecting organisations

Organisations in both private and public sectors currently adhere to data protection requirements under the Data Protection Act 1998. We will ensure that such requirements are, where appropriate, strengthened or amended to reflect the changing nature and scope of the digital economy. This will help organisations protect personal data, their reputation and their business by properly securing and managing data.

- *We will build accountability but with less bureaucracy.*
  The aim is to alleviate administrative and financial burdens on data controllers, but also make data controllers more accountable for the data being processed. Businesses must notify the ICO within 72 hours of a data breach taking place, if the breach risks the rights and freedoms of an individual. In cases where there is a high risk, businesses must notify the individuals affected.

[7] Although this general right may be subject to some exemptions in certain circumstances

- *We will help to reduce business exposure to risk of data protection breaches and the associated fines and reputational damage.*
  Organisations carrying out high risk data processing will be obliged to carry out an impact assessment to understand the risks involved and mitigation required to prevent inappropriate usage. Organisations must now prioritise personal privacy rights when handling personal data.

- *Simpler rules.*
  The rules will be consolidated to provide a clearer regime, which is fairer for data controllers and processors.

A tough regulator

The data protection regulator, the Information Commissioner, will retain existing powers and gain additional authority to impose greater sanctions in the event of data breach. The Information Commissioner's Office (ICO) will be empowered to take the following actions:

- Investigative powers - the ICO will continue to have the ability to request information from data controllers and processors, enter and inspect premises, carry out audits and require improvements.

- Civil sanctions - Currently the maximum fine the ICO can issue is £0.5m. Larger fines of up to £17m (€20m) or 4% of global turnover will be allowed, enabling the ICO to respond in a proportionate manner to the most serious data breaches.

- Criminal sanctions - The ICO or the Crown Prosecution Service and equivalent prosecutorial agencies in Scotland and Northern Ireland will continue to prosecute offenders. The most serious offences will become recordable[8]. Offences will be modernised to ensure that prosecutions continue to be effective and we will also create new offences to deal with emerging threats. In particular, we will:

    - Create a new offence of intentionally or recklessly re-identifying individuals from anonymised or pseudonymised data. Offenders who knowingly handle or process such data will also be guilty of an offence. The maximum penalty would be an unlimited fine.
    - Create a new offence of altering records with intent to prevent disclosure following a subject access request. The offence would use section 77 of the Freedom of Information Act 2000 as a template. The scope of the offence would apply not only to public authorities, but to all data controllers and processors. The maximum penalty would be

[8] Recordable offences are offences which are recorded on the Police National Computer, also known as PNC, database which can be disclosed as part of previous conviction or criminality checks.

an unlimited fine in England and Wales or a Level 5 fine in Scotland and Northern Ireland.
    - Widen the existing offence of unlawfully obtaining data to capture people who retain data against the wishes of the controller (even if the they initially obtained it lawfully).

- Protection for journalists and whistleblowers - The important role of journalists and whistleblowers in holding organisations to account and underpinning our free press will be protected by exemptions.

A bespoke regime for law enforcement purposes

Modern crime requires a modern response. We will provide a bespoke framework for our criminal justice agencies, tailored specifically to their needs, which will govern data processing for law enforcement purposes. It is vital that criminal justice agencies can work in dialogue, within borders and across them, to share information in order to protect the public and fight crime.

Our criminal justice agencies require a data protection framework that continues to allow them to tackle the changing nature of the threats we face - without compromising the world class data protection standards we expect. Amongst other requirements, we will introduce:

- A requirement for a mandatory Data Protection Officer (DPO). This is a new role and will advise data controllers on data issues, handle complaints and ensure compliance with the Data Protection Law Enforcement Directive.

- A requirement on data controllers to prove that requests by someone to obtain or verify information that is held about them is ‘manifestly unfounded or excessive before they are able to charge for the fulfilment of that request, or refuse altogether.

- A more prescriptive logging requirement applied to specific operations of automated processing systems including collection, alteration, consultation, disclosure, combination and erasure of data, so a full audit trail will be available.

- Clarity on the ability for international transfers to take place in a variety of circumstances, so critical data sharing can take place.

3. Implementing the Reforms

Overview

In the global digital economy, it is sensible for international frameworks to underpin our domestic data protection laws. There are three international instruments that form the core of the law in this area:

(i) The General Data Protection Regulation[9];
(ii) The Data Protection Law Enforcement Directive[10]; and
(iii) The Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data[11].

The proposed Data Protection Bill must be consistent with these instruments as they help ensure the safe flow of data between the UK and key markets, such as the US and EU.

(i) The General Data Protection Regulation

The GDPR, which becomes directly applicable on 25 May 2018, strengthens citizens' rights in relation to their personal data and facilitates business by simplifying rules for companies.

The GDPR will introduce new individual rights and new obligations on data controllers and processors.

New individual rights

- *Right to access your data* - The GDPR requires that data controllers provide individuals the first copy of the personal data undergoing processing free of charge. For any further copies requested, the controller may charge a "reasonable fee" based on administrative costs.

- *Data portability* – A new right to data portability, which allows for individuals to receive the personal data, which they have provided to a controller, in a structured, commonly used and machine-readable format, and to transmit them to another data controller. This may include:

    - Data collected through the tracking and recording of an individual (such as an app recording heartbeat or technology used to track browsing behaviour),
    - Raw data generated by a smart meter.

[9] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016
[10] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016
[11] ETS No.108

- *Right to be forgotten* – The GDPR widens the existing 'right to be forgotten', including the right for individuals to obtain erasure of personal data relating to them and the abstention from further dissemination of such data. The principle difference is a strengthening of the law from being applicable when substantial damage or distress is likely to be caused, to whenever a data subject withdraws their original consent for the data to be available, as long as it is no longer necessary or legally required for the grounds on which it was originally collected, or there are no overriding legitimate grounds for processing.

- *Legal remedy* – There is greater scope for enforcing rights under the GDPR. Where an individual is affected by an infringement of data protection rules, it should be possible for actions to be brought on behalf of similarly affected individuals by a representative entity (e.g. ombudsman, consumer or civil society bodies).

New obligations on data controllers and processors

- *Data breach notification* – The GDPR adds a requirement for data controllers to notify the supervisory authority (ICO in the UK) of personal data breaches, without undue delay, and within 72 hours where this is feasible, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of an individual.

- *Abolishing processing notifications* - The GDPR abolishes the current system requiring data controllers to notify the supervisory authority of their processing of personal data. Currently data controllers must notify the ICO of their data processing activities and pay a fee.

- *Data Protection Impact Assessments* - A requirement that data controllers or processors must undertake a data protection impact assessment on data processing which presents high risks.

- *Data protection officers* - A requirement that data controllers or processors must designate a data protection officer if they are a public authority or body (except for courts); or their core activities include processing operations which are regular and systematic on a large scale or including processing special categories of personal data and data relating to criminal convictions or offences.

- *Administrative sanctions* – A new range of administrative sanctions for a wide range of infringements of the Regulation are introduced by the GDPR. Penalties of up to £17m (€20m) or 4% of global turnover.

The GDPR, which was adopted by the European Union in 2016, will automatically come into force in all EU Member States from 25 May 2018. The GDPR will have

"direct effect". This means that it confers rights on individuals which the courts are bound to recognise and enforce.

The GDPR only applies, however, to data which is inside an area of exercised EU legal competence. This means that our own laws will need to apply data protections to other areas, and we intend to apply substantively the same standards to all general data, in order to create a clear and coherent data protection regime.

The Data Protection Bill

We are determined to ensure that the GDPR best supports UK interests - for citizens and businesses. The GDPR requires some modification to make it work for the benefit of the UK and the Data Protection Bill will make the necessary changes. In particular, the Bill will:

- Exercise the available derogations in the GDPR that the UK government negotiated. This will allow:
    - The implementation of key government commitments including, the ability to require social media platforms to, on request, delete information held about them at the age of 18.
    - A simpler shift for both business and consumers as we will retain many of the enablers of processing essential to all sectors of the economy, from financial services to academic research, under the new legislation.

- Apply the new data protection standards to all general data, not just areas of EU competence.
    - We are leaving the EU and businesses need a single standard under which they can operate. We do not want differing standards for legal areas which previously came under EU competence. The Bill will ensure that quality standards are also simple to apply.

- Repeal the Data Protection Act 1998.
    - When the GDPR takes effect it will be confusing for individuals, businesses and the courts if we do not adjust our domestic law to remove inconsistencies. The Data Protection Bill will make the necessary repeals to ensure clarity of roles and responsibilities for all involved.

Call for views

Before deciding how to implement the GDPR, we recognised that it was vital to listen to the views of those organisations and individuals who may be affected by our decision.

Consequently we took two key steps. Firstly, we spoke, informally, to wide-ranging stakeholders. This enabled us to form a broad understanding of different views.

Secondly, we invited any interested person or organisation to give us their views through a "call for views" exercise from 12 April 2017 until 10 May 2017.[12] All stakeholders with an interest in data protection were encouraged to share views on any or all of the derogations, which were categorised by a number of distinct themes. Any supporting evidence was welcomed. This made it easier for stakeholders to understand the key ways in which the exemptions relate to each other.

The "call for views" proved extremely useful: the government received 170 responses from organisations in total, representing wide-ranging points of view. For example, responses were received from not only the technology and legal sectors, but also local government and consumer protection groups. Private individuals also provided helpful contributions. Overall, the "call for views" enabled government to achieve a fuller understanding of the potential impact of each of the exemptions. In some cases late responses contained new points of substance, and we endeavoured to incorporate these into our policy development where possible.

We have published the responses we have received to the "Call for Views" in full on GOV.UK. A list of those organisations that responded is at the end of this document.

[12] https://www.gov.uk/government/consultations/general-data-protection-regulation-call-for-views

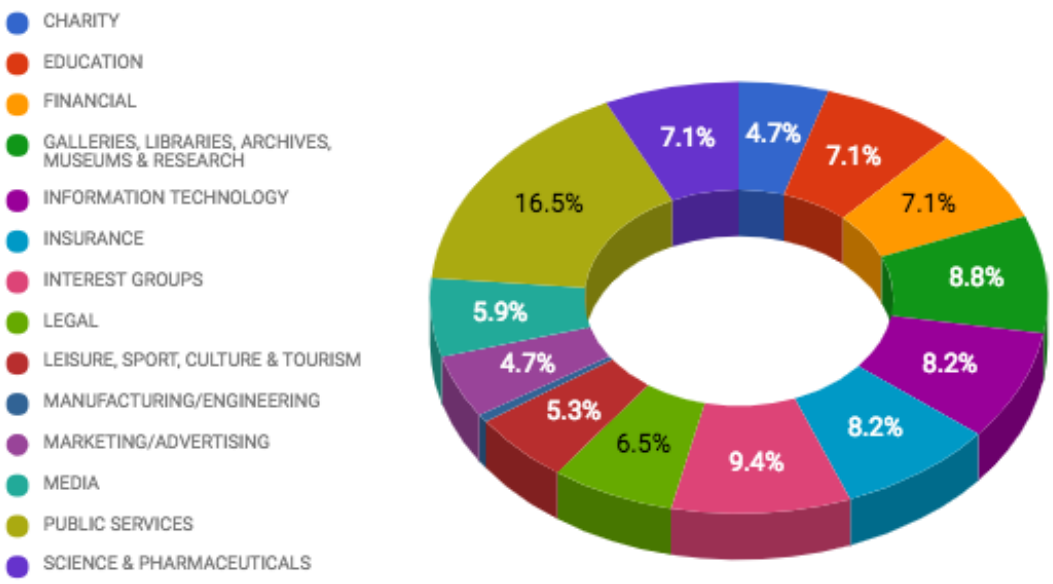

Fig: Responses to the Call for Views by sector

In considering each derogation, we were careful to ensure that it struck a balance between, on the one hand, protecting UK citizens' rights and, on the other hand, enabling data to flow freely - which is good for businesses and society as a whole.

Notable derogations

Giving consent to process data and protecting children online

The GDPR makes clearer the circumstances where controllers can rely on consent when processing personal data. Of course, persons giving consent need to have a certain level of understanding of what they are being asked which is why the GDPR specifies that parents or guardians must give consent to personal data processing on behalf of young children using information services. The GDPR allows the UK to set that threshold for the minimum age at which a child can consent to data processing to any age between 13 years and 16 years. Currently there are no overall rules, but where they exist, the equivalent age in the UK is 12[13].

Child online safety is one of the top priorities for this government. As announced in the Queen's Speech, the government will establish a Digital Charter, which will aim to make the UK the best place to start and run a digital business and the safest place in the world to be online. As part of the Digital Charter work has already begun on an Internet Safety Strategy with the aim of making online environments safer children and young people.[14] We are working with internet service providers, app makers,

[13] ICO guidance states: "Some form of parental consent would normally be required before collecting personal data from children under 12", Personal information online code of practice, July 2010
[14] https://www.gov.uk/government/news/government-launches-major-new-drive-on-internet-safety

social media providers and others on the strategy which will be taken forward as part of the charter. We expect responsible websites to have minimum age rules and policies to ensure that children are not exposed to inappropriate content.

No respondents to our call for views expressed a firm view that the minimum age to consent to data processing should be set higher than age 13. We did receive submissions that any age control should be better enforced, which we will consider as part of our work on the Internet Safety Strategy. Age checks at age 18 are increasingly commonplace online but at that age it is possible to check credit records, driving records and electoral records. These do not exist for children aged 13 to 16 and most websites therefore start by asking questions, building trust and then investigating unusual behaviour or complaints.

Setting an age threshold is not the only - or best - way to protect children's personal data. The Internet Safety Strategy will show a better way, building a shared responsibility between internet service providers, app makers, social media providers and others. Indeed, the GDPR introduces other rights which will serve this purpose. A good example is the new requirement that privacy notices - which set out how an organisation plans to use the personal data it collects - be in a format which children can understand.

Social media already plays a fundamental role in many teenagers lives and online platforms and communities present significant opportunity and benefits to children and young people. Through our work on online safety, the government aims to give children the tools they need to maximise these opportunities, including through education and awareness, to build their digital literacy skills, and stay safe online. By placing such a high priority on online safety, we expect businesses, including social media companies, to step up to their responsibilities in creating safer spaces for children and young people to enjoy their time online.

In view of all these considerations, we will legislate to allow a child aged 13 years or older to consent to their personal data being processed.

Processing criminal conviction and offence data

The GDPR only permits bodies vested with official authority to process personal data on criminal convictions and offences. This position acknowledges the highly sensitive nature of such data.

However, GDPR does allow the UK to legislate to allow other bodies to process this category of personal data. For example, UK legislation could permit a private or third sector employer to obtain details of criminal convictions in order to carry out a criminal records check.

Current UK law allows all organisations to process personal data on criminal convictions and offences in certain specified circumstances. This has had, in practice, a number of key benefits; for example organisations have been enabled to

protect themselves from potential criminal acts and to safeguard children and vulnerable adults; employers have found it possible to perform accurate criminal records checks; and the underwriting of driving insurance has been facilitated. The government believes that, should this right for a wider range of organisations to process criminal convictions and offences data be removed, there would be a significant, negative impact on UK interests.

In view of this, and to preserve continuity with an aspect of current data protection which has been proven to work well in practice, we will legislate to extend the right to process personal data on criminal convictions and offences so as to enable organisations other than those vested with official authority to process criminal convictions and offences data. We will take a similar approach to that taken for the processing of special (i.e. sensitive) categories of personal data.

Automated individual decision-making

According to the GDPR, an individual has the right not to be the subject of automated decision making including "profiling". This may include, for example, an individual receiving an unfavourable credit rating, which is decided by way of a purely automated process.

The GDPR also allows exemptions where suitable measures are put in place to safeguard the individual's rights, freedoms and legitimate interests. It is important for an individual to have recourse in the event that they are subject to an unfavourable automated decision. There are also legitimate functions which are dependent on automated decision making. For example, a bank, before agreeing to provide a loan, would be entitled to check the creditworthiness of an applicant. In this context, an automated credit reference check would be an appropriate means of achieving this outcome.

In view of this, we will legislate to implement this exemption with a view to ensuring legitimate grounds for processing personal data by automated means. Individuals will have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to them which is based solely on automated processing and which produces legal effects or similarly significantly affects them, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention.

Freedom of expression in the media

A free media is vital to democracy and it is crucial that journalists are able to hold power to account without fear or favour. The GDPR provides for journalistic exemptions to certain areas of data protection to allow for journalistic activity in the public interest to be carried out. The new Data Protection Bill will strike the right balance between freedom of expression of the media and the right to privacy for individuals.

There are eight main principles in the Data Protection Act 1998 that organisations need to comply with. Under section 32 of the Act, exemptions exist for personal data which are processed for special purposes if the processing is undertaken with a view to publication, that publication is in the public interest, and compliance with the principle is incompatible with the special purposes.

We believe the existing exemptions set out in section 32 strike the right balance between privacy and freedom of expression. While some respondents in the government's Call for Views argued for a wider exemption, particularly media organisations, the government believes the current provisions allow for investigative journalism in the public interest while protecting individuals and their personal data.

The government intends broadly to replicate section 32 of the Data Protection Act 1998. The main difference will be to amend provisions relating to the ICO's enforcement powers to strengthen the ICO's ability to enforce the re-enacted section 32 exemptions effectively.

Research

The UK has many world leading universities, research establishments and museums. They handle vast amounts of information and need to continue to operate in a way that protects information but is not burdensome or inhibits future innovation and discovery.

The GDPR requires organisations to comply with specified obligations in relation to an individual's personal data. Such obligations include, for example, the requirement that inaccurate personal data, upon notification, be rectified without delay as well as rights of access.

The GDPR, however, also allows the UK to legislate to allow scientific or historical research organisations, organisations which gather statistics or organisations performing archiving functions in the public interest, to be exempted from such obligations. However, this will only be the case if compliance would seriously impair these organisations' ability to carry out research, archiving or statistics-gathering activities. For example, it may be that only by archiving inaccurate data is it possible to audit a decision-making process which led to an unfavourable outcome. Should all such data be rectified, the opportunity to learn lessons, and prevent a similar outcome in the future, may be severely diminished. A further example would be that statistical data may be compromised, leading to inaccurate conclusions, if individuals' personal data is removed from the statistical "pool".

The government will legislate to exercise this exemption in order to ensure that the UK continues to be a centre for groundbreaking research. We will ensure that research organisations and archiving services do not have to respond to subject access requests when this would seriously impair or prevent them from fulfilling their purposes. Research organisations will not have to comply with an individual's rights to rectify, restrict further processing and, object to processing where this would

seriously impede their ability to complete their work, and providing that appropriate organisational safeguards are in place to keep the data secure.

(ii) Law Enforcement data protection

As the world becomes increasingly connected, the nature of crime is also changing. This presents both opportunities and challenges: data and data sharing can provide powerful tools to prevent and detect crime whilst, at the same time, the internet enables offenders from anywhere in the world to target UK citizens and commit offences.

In this context, it is vital that criminal justice agencies, within the UK and internationally, can work together, sharing information in order to keep the public safe. However, it is equally important that such data sharing is subject to appropriate safeguards.

The Data Protection Bill will ensure there is a framework for those handling data for law enforcement purposes. The GDPR does not cover the processing of personal data for "prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security". The Data Protection Bill will implement into UK law the EU Data Protection Law Enforcement Directive which will extend to domestic law enforcement as well as cross-border.

This Bill will also ensure there is a framework for the handling of personal data for activities falling within Chapter 2 of Title V of the Treaty on European Union (common foreign and security policy). The GDPR does not cover the processing of personal data for national security. The Data Protection Bill will ensure that there is a suitable framework for the processing of personal data for these purposes.

<u>The Data Protection Law Enforcement Directive</u>
The Data Protection Law Enforcement Directive (DPLED), in contrast to the GDPR, is not "directly applicable" EU law. This means that the UK must implement its provisions prior to 6 May 2018. However, in order to ensure a consistent, comprehensive and forward-looking framework for data protection in the UK, the Data Protection Bill will write into UK law both the GDPR exemptions and the DPLED provisions for both cross border and domestic law processing of personal data.

The Bill will create a bespoke regime for law enforcement data protection, tailored to meet the needs of not only the police, but also prosecutors and other criminal justice agencies - including, in various circumstances, organisations as diverse as Her Majesty's Revenue and Customs, the Environment Agency, or the Driver and Vehicle Licensing Agency.

The Bill will help to cement the UK's reputation for upholding the highest standard of data protection. The UK successfully negotiated to ensure that the finalised DPLED

would allow the unhindered flow of data whilst providing safeguards to protect personal data. Consequently, the Bill will represent a good outcome for UK citizens and criminal justice agencies alike.

New Powers and Increased Protection

Increased cross-border data exchanges are key to tackling the threats posed by terrorism and organised and online crime. Recent terror attacks, both at home and abroad, demonstrate the need for international cooperation to tackle these threats.

The Bill will reform and strengthen the rules on international data transfers. It provides a clear framework which enables UK law enforcement agencies to transfer data to counterparts in partner countries or international organisations.

Whilst it is crucial that criminal justice agencies have at their disposal all the powers they need to fight crime and protect the public, the government recognises that the personal data processed for law enforcement purposes can be very sensitive. Due to this, it is equally important that such agencies must operate within the parameters established by a clear and proportionate framework. The government believes that the Bill will provide the flexibility which criminal justice agencies require and maintains leading standards in data protection and privacy.

The Bill will tighten data protection requirements. In particular, it makes it easier for individuals to access their own data and to understand their data protection rights. Furthermore, if an individual requests information on the ways in which their personal information is processed, the data controller will be required to provide that information free of charge.[15]

The Bill will also set out to reassure citizens by promoting the concept of "privacy by default and design". This is achieved by giving citizens the right to know when their personal data has been released in contravention of the data protection safeguards, and also by offering them a clearer right of redress. In order to provide clear audit trails, databases which process personal data will be required to adhere to more rigorous logging requirements.

A Consistent Approach

Although the DPLED is focused on cross-border data sharing, the government has decided that, in order to ensure consistency and certainty for criminal justice agencies, the standards which the DPLED establishes will be extended to all domestic data processing for law enforcement purposes. This demonstrates our commitment to staying at the forefront of data protection standards.

[15] This obligation will not apply if the request for information is manifestly unfounded or excessive.

(iii) National Security Data Processing

National security is outside of scope of EU law and, consequently, the processing of personal data for national security purposes is not addressed by either the GDPR or DPLED.

Nevertheless, it is vitally important that UK data protection law remains up-to-date and in-line with international standards, whilst also ensuring that the UK intelligence community and others can tackle existing, new and emerging national security threats.

In view of this, the UK plans to legislate to provide for a distinct data protection framework, specifically for national security purposes, which builds on, and modernises, the existing regime. It will be based on the revised Council of Europe Convention for the Protection of Individuals with Regards to Automatic Processing of Personal Data (Convention 108). The Council of Europe, founded in 1949, has 47 member states, and is not one of the institutions of the EU. The UK will continue to be a member of the Council of Europe after we have left the EU.

The Council of Europe is a distinct, stand-alone body. Its role is to uphold human rights, democracy and the rule of law across Europe. The revised standard is currently in draft and as a founding member of the Council, the UK has been taking an active role in negotiations to ensure it aligns with national priorities. However it will introduce data protection standards which reflect the huge growth in data and changes in technology, and will establish a number of principles, key to ensuring that data is processed, not only lawfully, but ethically. As now (see section 28 of the Data Protection Act 1998), a number of exemptions from certain data protection principles and other provisions of the revised Convention 108 will be necessary for the purposes of protecting national security.

This framework will be forward-looking with a view to being in-line with anticipated future international standards, thus demonstrating that the UK remains “ahead of the game” when protecting citizens’ data.

4. Looking Ahead

Cybersecurity and Data Protection

Effective data protection in part relies on organisations adequately protecting their IT systems from malicious interference. Recent cyber security incidents, however, have made it clear those businesses of all sizes and sectors face cyber risks to their IT systems and the data these systems hold[16].

The National Cyber Security Centre have published '*10 Steps to Cyber Security*' - detailed guidance on how organisations can protect themselves from cyber security threats[17]. Further, the Cyber Essentials accreditation scheme offers a mechanism for organisations to demonstrate that they have taken basic technical measures to protect their systems against the most common cyber threats.

The government's *Cyber Security Regulation and Incentives Review*[18] concluded that the implementation of the new data protection law should result in significant improvements to the management of cyber security risks. Indeed, evidence gathered in the course of the *Review* indicated that the increased financial sanctions applicable for data breaches, and the introduction of aggravating and mitigating factors, will result in improved cybersecurity practices in the UK.

The new law's requirement that data breaches be reported will also contribute to a richer source of data on cybersecurity breaches. This will be critical in allowing government to develop robust and effective cybersecurity policy in the future. This will make the UK an even safer place for everyone - individuals, businesses and other organisations - to go online.

The government is also working with the ICO and the National Cyber Security Centre to ensure that UK organisations understand their new data protection responsibilities and, crucially, are incentivised to improve their cybersecurity behaviours ahead of implementation.

Data, Trade and the European Union

Strong data protection law and appropriate safeguards enable businesses to operate across international borders.

The ability for data, both personal and non-personal, to flow across borders is essential for global trade - in both goods and services. Indeed, digitally-deliverable

[16] https://www.ncsc.gov.uk/report/cyber-threat-uk-business
[17] https://www.ncsc.gov.uk/guidance/10-steps-cyber-security
[18] https://www.gov.uk/government/publications/cyber-security-regulation-and-incentives-review

services comprise approximately 75 percent of products traded and delivered online.[19] Global flows, as a whole, have increased world GDP by at least 10 percent, with the sum total of around £5 trillion in 2014 alone. Data flows account for around £1.7 trillion of this effect which means that data flows are exerting a larger impact on growth than traditional goods flows.[20]

Unhindered flow of data, therefore, is essential to the UK forging its own path as an ambitious trading partner. That is why the government will be seeking to ensure that data flows between the UK and the EU, and also appropriately between the UK and third countries and international organisations, remain uninterrupted after the UK's exit from the EU. Cooperation with the UK's law enforcement and security partners, both in Europe and beyond, will also remain a priority.

[19] United States International Trade Commission (2014), Digital Trade in the U.S. and Global Economies, Part 2, https://www.usitc.gov/publications/332/pub4485.pdf

[20] McKinsey Global Institute (2016), Digital globalization: The new era of global flows, http://www.mckinsey.com/~/media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi-digital-globalization-full-report.ashx

Annex - Organisations that responded to the Call for Views*

Advertising Association

AFME - Finance for Europe

Alan Turing Institute

Amber Information Consulting

Archives and Records Association (UK & NI)

Archives Wales

Art Fund

Association of British Insurers

Association of School and College Leaders

Association of Show And Agricultural Organisations

Aviva

AXA UK Plc

Bar Council

Bassetlaw District Council

Bates Wells Braithwaite

BBA

BGL Group Limited

Big Brother Watch

British Academy

British and Irish Law Education and Technology Association

British Broadcasting Corporation

British Library

British Medical Association

British Toy & Hobby Association

CACI Ltd

Callcredit Information Group

CBI

Channel 4

Charity Commission - England and Wales

Charity Tax Group

Chartered Institute of Credit Management

Chartered Institute of Journalists

Children's Charities' Coalition on Internet Safety

Children's Commissioner for England

Children's Commercial Media Literacy

Cifas

CMS Cameron McKenna Nabarro Olswang LLP

Cock, Burns & Burrows LLP

Cohort & Longitudinal Studies Enhancement Resources (CLOSER)

Common Sense Privacy Ltd

Companies House

Cooperative Group

Coop Insurance

Council for Advancement and Support of Education Europe

Council of Mortgage Lenders

Cultural Heritage Institutions Privacy Alliance

Cunningham Lindsey

Data analysts User Group

Defend Digital Me

Department for Work and Pensions

Direct Marketing Association UK

Dun & Bradstreet

Economic & Social Research Council

EEF, the manufacturers' organisation

Electronic Frontier Foundation

Equifax Limited

Essex County Council

Experian

Facewatch Ltd

Factiva Limited

Finance and Leasing Association

Freedom of Expression Group

FSB - experts in business

Future Care Capital

Gambling Commission

General Medical Council

General Pharmaceutical Council

Glasgow City Council

Greenwich Foundation for the Old Royal Naval

Griffin House Consultancy Limited

Group Risk Development

Guardian News & Media

Hammersmith Medicines Research Ltd

Hampshire County Council

Health and Research Organisations (Wellcome Trust)

Health and Social Care GDPR working Group

Henley Business School

Her Majesty's Land Registry

Heriot-Watt University

Heritage Alliance

Horwich Farrelly Solicitors

Imperial College NHS Healthcare Trust

Imperial War Museum

Information and Records Management Society

Information Commissioner's Office

Information Security Know How Ltd

Insurance Fraud Bureau

Institute of Practitioners In Advertising

Internet Advertising Bureau UK

Intu properties plc

Investment & Life Assurance Group

ISBA - Voice of British Advertisers

ITM Limited

JISC - digital technology

Law Society

Leeds City Council

Lewis Silkin LLP

Liverpool Victoria Friendly Society

Market Research Society

medConfidential

Media Lawyers Association

MIB

More Partnership

Munich RE

Museum of London

National Association of Business Crime Partnerships

National Library of Scotland

National Portrait Gallery

National Records of Scotland

National Society for the Prevention of Cruelty to Children

Natural History Museum

NatCen

NEC Europe Ltd

News Media Association

NHS Digital Strategic IG

Office for National Statistics

Open GI Limited

Open Rights Group

Oxford Internet Institute

PA Consulting

Plymouth City Council

Privacy International

Professional Players Federation

Public Record Office of Northern Ireland

QuintilesIMS

RAFBF

Registry Trust Limited

RELX Group

Remote Gambling Association

Reporters Committee for Freedom of the Press

Research Libraries UK

Royal College of Physicians

Russell Group

Salford City Council

Samaritans

Scottish Courts & Tribunal Service

Scottish Government

Sheffield City Council

Somerset County Council

Southend on Sea Borough Council

Sport England

Sports Betting Group

Stone King LLP

Tech UK

Thomson Reuters

UK Statistics Authority

United Kingdom Accreditation Service

Universities UK

University College London

University of Birmingham

University of Cambridge

University of Keele

University of Manchester

University of Southampton

Unlock

VIVID (previously First Wessex and Sentinel housing)

Water UK

Wealth Management Association

West Bromwich Building Society

Western Sussex Hospitals NHS

Which?

Wifi SPARK Ltd

YOTI

Young Scot - 5 Rights Youth Commission

ZigZag Global Ltd

*5 organisations requested to remain anonymous

Department for
Digital, Culture
Media & Sport

4th Floor, 100 Parliament Street
London SW1A 2BQ
www.gov.uk/dcms

ISBN: 978-1-911619-00-0